BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing	)	
The Telephone Consumer Protection	)	CG Docket No. 02-278
Act of 1991	)	CC Docket No. 92-90
	)	
	)	
	)	
	)	

COMMENTS OF PRIVACILLA.ORG

Introduction

Privacilla.org is a Web-based think-tank devoted to privacy as a public policy issue. Privacilla (http://www.privacilla.org) attempts to capture privacy from top to bottom, discussing important privacy concepts, policies, and proposals. Privacilla covers privacy from government and privacy in the private sector, including online, financial, and medical privacy. Privacilla has an explicit pro-technology, free-market perspective and a belief that the best way to serve consumers' true interests is by harnessing the energy of markets in their favor.

As the Federal Communications Commission's Notice of Proposed Rulemaking reflects, some means of contacting and communicating with consumers can and do outstrip their desires to be communicated to. Autodialers, and particularly predictive dialers, can be overly communicative. The present rulemaking regards suppressing communications consistent with both the interests of the public and with constitutional limitations on government power.

An increasing array of technologies exists to serve the interests pursued by the Federal Communications Commission in this rulemaking under the authority of the Telephone Consumer Protection Act. The Commission should consider the growing role of technology in suppressing communications precisely consistent with consumers' desires. The growing availability of technologies for this purpose undermines regulatory solutions both in terms of their utility and in terms of their constitutional viability under the First Amendment.

The Commission should take the concept of "privacy" well in hand in this rulemaking. Though privacy is mentioned throughout the TCPA and this rulemaking, the actual interest pursued through the policies at issue is freedom from annoyance, which lies only on the outskirts of privacy as that concept is recognized in American law. At the same time, instituting a do-not-call list should be recognized as a fundamentally anti-privacy choice. This does not end consideration of do-not-call listing, but participants in

a do-not-call list should be made aware that they do not gain privacy, but rather give up privacy in order to be relived of some annoyance.

Consumer-Empowering Technologies Are Increasingly Available

The Commission is wise to inquire about the availability of technologies that allow consumers to avoid receiving unwanted telephone solicitations (NPRM ¶ 21). This inquiry, however, appears limited in ways that render the Commission's consideration of the issues too narrow. Just as the marketplace for telemarketing has changed since 1992 (NPRM ¶ 7), the marketplace for telemarketing suppression has changed.

The Commission should consider all technologies that advance consumers' interests in suppressing communications — not just "network" technologies. (It is unclear what exactly a "network" technology is, but the Commission's study of technology should not be artificially limited.) The TeleZapper (http://www.telezapper.com), for example, is a technology residing at the edge of the wireline telephone network. It sends a tone at the outset of any call indicating to autodialers that the number reached is out of service. Typically, this ends a call immediately and removes the number from any list maintained by the autodialer. Many other highly relevant non-"network" technologies are discussed below.

The Commission should also consider technologies that allow consumers to avoid all unwanted telephone calls, of which telephone solicitations are a subset. Cellular

phones can be turned off by their users at night, for example, giving consumers precise power over the hours at which calls are received, including commercial solicitations. As the Commission has found, cellular phones are increasingly the primary phone for many consumers. In addition, traditional phones in more and more homes offer consumers control over the operation and volume of the ringer, which can control the intrusiveness of calls at the consumer's discretion. A benefit of answering machines — whose use undoubtedly continues to grow — is that they allow consumers to screen calls and pick up the ones they want. The list of call avoidance option goes on.

The Commission need not operate on the assumption that consumers will always expect to answer every incoming call. Many consumers have already adopted the effective, though imperfect, practice of not answering the phone when they do not want to be bothered. Consumer expectations are dynamic. The offense of receiving unwanted calls, which animated the Telephone Consumer Protection Act when telemarketing was relatively new, is giving way to a practical expectation, chiefly among the young, that some calls are worth answering and some calls are not.

Consider Innovation and the Interests of Taxpayers

The Commission should also consider technologies and practices that have yet to be invented or deployed, but that easily could emerge given the current state and direction of technology. For example, if unwanted calling is truly a demand of

consumers, telephone service providers or gadget makers may soon offer an incoming call option or device that directs calls to voice mail unless the recipient has "white-listed" the caller's number. Friends, relatives, business colleagues, and (with intelligent planning) emergency callers could ring a phone at any time. Other callers, and those who block caller ID, would be free to leave a voice mail for the consumer to pick up at his or her leisure. Phones could also have distinctive rings depending on whether a call is from a "white-listed" number or not. Unless regulation thwarts it, voice over Internet protocol should make available an even broader and entirely customizable array of such options to consumers.

The TCPA and government do-not-call listing compete against innovative new technologies, the market, and the best interests of taxpayers. By offering a partial solution to the problem of intrusive phone calling, they suppress consumer demand for technical and market solutions that would otherwise emerge. Overlapping regulatory processes like this NPRM, the previous one, and the concurrent one at the Federal Trade Commission are paid for by all taxpayers regardless of their interest in suppressing telemarketing. All taxpayers must also pay continually for regulatory enforcements and operation of the courts to adjudicate both public and private remedies.

Technical solutions offered in the marketplace, on the other hand, are paid for by precisely the consumers who want them at precisely the levels they want them. And because consumers always demand more for less — and can get it when there is

competition — communications suppression will be delivered more efficiently and inexpensively by diverse and changing markets than by unitary and static government solutions.

The Commission should not irrationally blind itself to existing and coming communications suppression technologies. Used by consumers in the marketplace, they have none of the First Amendment problems associated with regulatory solutions, they generally have less of the time-lag that regulatory solutions have, and they have far more precise delivery of specific communications suppression to specific consumers than bureaucratic regulation.

Rather than attempting to reinvigorate bureaucratic solutions, the Commission should play a productive role as a convener and taskmaster for the telecommunications and technology companies who, combined, have the ability and the economic interest to give consumers the control that they actually want. The Commission should ensure that regulation does not impede the ability of telecommunications providers to suppress communications consistent with the interests of their customers. And the Commission should educate the public about the options available to them now, and those coming, in the marketplace.

Government Suppression of Communications Suffers Growing Practical and Constitutional Weakness

The increased availability and possibility of consumer-driven communications suppression technologies put the TCPA generally, and do-not-call listing specifically, on weak ground in several respects. As consumer-protection policy, telemarketing rules and government do-not-call listing are becoming increasingly clumsy bureaucratic contraptions. New technologies, aggressive consumerism, and realistic consumer expectations will tend to solve the problem of unwanted telemarketing. Bureaucratic regulation will tend to institutionalize that problem.

Just as importantly, advancing technology is pushing telemarketing rules and government do-not-call listing further and further from constitutional permissibility under *Central Hudson*. (NPRM ¶ 12)

As consumers become more able tailor on their own what communications they receive, blanket regulation of communications will advance less and less the interest of any part of the public in being free from unwanted communications. To illustrate: If all consumers interested in being rid of telemarketing adopted technologies that suppressed it consistent with their preferences, limitations on speech under the TCPA would *only* prevent communication from reaching consumers whose preferences ranged from indifferent to appreciative of telemarketing. In such conditions, regulation of speech under the TCPA would not materially advance the interest of any part of the public in

being free from unwanted communications. Nor would it be tailored to serve that interest because it would only suppress communication that was wanted by, or a matter of indifference to, consumers. As the public progresses to those conditions through adoption of technology, the TCPA will grow increasingly questionable as a constitutional matter — and it should.

The Commission Should be Clear on the Issue of "Privacy"

The purpose of this comment, though, is not to discuss communications suppression technologies. Rather, it is to make two points about privacy in relation to the NPRM.

First, the Commission should consider very carefully what precise interests are advanced by limitations on marketing communications. Unwanted calling is an annoyance and an inconvenience that resides at the outskirts of "privacy" as an established legal concept. This is very important to the Commission's obligation under *Central Hudson* to advance a substantial interest in any regulation that suppresses speech.

Second, true privacy is actually threatened by do-not-call listing. Databases residing in the hands of governments are more serious risks to privacy than data anywhere else. This is because governments have unique powers to change the terms under which information is held and used. Do-not-call listing is a small, incremental loss

to privacy, but it is nonetheless an erosion of privacy too ironic to let pass in a regulation often touted as "privacy" protection.

Privacy is a goal that is often sought in our public policy, but it has been singularly elusive. This is largely because no settled definition of the concept has emerged. In the absence of definition, governments and agencies pursuing privacy have aimed themselves at amorphous and sometimes conflicting goals, and they often have had no basis on which to judge whether they have succeeded at reaching them. This is the situation faced by the Commission if it does not come to grips with "privacy" in this rulemaking.

To improve the quality of privacy policy-making, Privacilla.org has created a definition of the term "privacy" that captures the concept and allows other concepts in information policy to be distinguished. Our definition of privacy is this: *Privacy is a subjective condition that individuals enjoy when two factors are in place — legal ability to control information about oneself, and exercise of that control consistent with one's interests and values.*

Importantly, privacy is a subjective condition. This means that individuals determine its contours for themselves based on their own highly personal wants and needs. Through experience, upbringing, and culture, each person develops a sense of privacy that is his or her own. One person can not tell another what his or her sense of

privacy should be. Nor can legislators or regulators determine for an entire society what information practices deliver privacy to the people in it.

The first factor — legal power to control the release of information — goes to the existence of choice, not how pleasant the choices are. In the private sector, people almost always have the ability to control information about themselves. By declining to deal with others or engage in commercial transactions that have unsatisfactory consequences for information, they can decide absolutely who receives information about them. A variety of laws like contract, trespass, burglary, and battery enforce people's decisions to limit the access others have to information about them. Though it is not always easy to use, the existence of legal power to control information satisfies the first factor.

When dealing with governments, people rarely have legal power to control information. The data necessary to collect taxes, deliver benefits, and police citizens is collected by force of law. Data collected and held by governments — even if submitted voluntarily and confidential "by law" — may be deemed categorically *un*private because governments have the power to change the terms under which information is held and used. This is why government can fairly be called the greatest threat to privacy. No slight is intended to the good motives of public servants when the observation is made that loss of privacy is a cost of government.

Exercising control of information — the second factor that delivers privacy — relies on an educated and aware population pursuing their own interests in all their

interactions and in the marketplace. We cannot presuppose what consumers want in terms of privacy and publicity. Many consumers are unaware of how the Information Economy works, and the fact that they are a part of it. Other consumers have made rational decisions to share information in exchange for lower prices, convenience, customer service, customization, and other benefits. Only educated, empowered, and responsible consumers can maintain privacy at the level and on the terms they want it. They do this by going where they want, speaking to whom they want, and transacting with whom they want on the terms they want.

Privacilla's definition of privacy is rooted deeply in privacy law as it has developed in the United States over the last 100-plus years.[1] As is well known, the foundation of privacy as a concept in American law is an article called *The Right to Privacy*, published in the 1890 Harvard Law Review. The authors of the article, Samuel D. Warren and Louis D. Brandeis, were concerned with the rise of newspapers, photography, and other technologies that have the potential to expose people's images and personal information to the public. Warren and Brandeis argued that the next step in evolving legal protections for the individual should be explicit protection of privacy. The two compared the contours of explicit legal privacy protection to the law of defamation, to physical property rights, to intellectual property, and to the law of contracts.

---

[1] *See The Privacy Torts*:How U.S. State Law Quietly Leads the Way in Privacy Protection, Privacilla.org (July 2002) <http://www.privacilla.org/releases/Torts_Report.html>.

Their key concern was with publicity given to sensitive personal information — undesirable and embarrassing scrutiny of private life by the press and public. (Warren and his family, notable Boston "blue bloods," had been embarrassed and annoyed by newspaper coverage of their lives.) Privacy as discussed by Warren and Brandeis did not extend to matters that were of legitimate public or general interest. And publication of facts by the individual concerned, or with that person's consent, cut off that person's right to privacy in that information.

In 1960, eminent legal scholar William L. Prosser documented how privacy as a legal concept has come to constitute four distinct torts. That is, a person whose privacy has been invaded in any of four different ways can sue the invader for damages. These torts still exist today, and are roughly contoured as follows:

- Intrusion upon seclusion or solitude, or into private affairs;
- Public disclosure of embarrassing private facts;
- Publicity which places a person in a false light in the public eye; and
- Appropriation of one's name or likeness.

Prosser was not totally enamored with the privacy torts. The link among them — the idea that people have a right "to be let alone" — is slightly tenuous for legal theory. Prosser warned that the different ways each branch of the tort might apply could easily lead to confusion.

The one branch of the privacy torts that has relevance to the Telephone Consumer Protection Act is the "intrusion" tort. This branch has its foundation in wrongful entry upon places were private life is being conducted. An early precursor, for example, was a case involving a man's entry into a room where a woman was giving birth. The principle has been carried beyond places and belongings and an intrusion tort may occur when someone eavesdrops using microphones or wiretaps or when someone peeps through the windows of a home.

An intrusion probably has not occurred when someone makes excessive noise, exhibits bad manners, or makes obscene gestures. The intrusion tort is not implicated when the matters observed can not be accurately called "private," as when someone is observed or photographed on a public street.

Conceived as information policy, the intrusion tort can be said to give a cause of action to someone who has taken ordinary steps to control information about him or herself, but who finds it defeated by the unusual or outrageous behavior of others. The woman intruded upon while giving birth, for example, had reasonably protected information about her appearance and condition by retreating to a closed room for the purpose of childbirth. By strong custom and by implicit promise, she was joined there only by people with a role in her aid and an obligation to remain silent or discreet about the things they observed. The man entering the room without permission, and not subject

to these conditions wrongly defeated her exercise of control over sensitive personal information, and invaded her privacy.

On its outskirts, the intrusion tort more closely resembles harassment or stalking. Repeatedly phoning a person or trailing a person in public have less to do with divesting them of control over information as divesting them of peace of mind. These behaviors do not fit too comfortably in the intrusion branch of the privacy torts.

The Interest Pursued by the TCPA is not Privacy, but Rather Freedom From Annoyance

Unwanted telephone solicitation by many different parties certainly can be disconcerting and it annoys many people, but it probably resides beyond the legal concept known as privacy. It is probably best treated as the exhibition of bad manners. It is rude to call people about things they are not interested in, and it is rude to hang up on them without speaking.

In the best analysis, the interest pursued by the Telephone Consumer Protection Act and by the Commission in this rulemaking is relief from the annoyance of the rudeness inherent in unwanted telephone calls. The TCPA uses the term "privacy" several places. For example, it instructs the Commission to consider rules regarding consumers' "privacy rights to avoid receiving telephone solicitations to which they

object."[2] But the use of the term "privacy" in this instance is essentially hortatory. It does not convert the interest in being free from annoyance into "privacy" any more than declaring the moon to be made of green cheese converts frozen rocks and dust in space into dairy products.

Consider calls made to series of numbers at random. These rely on no personally identifiable information whatsoever. Characterizing such calls as privacy invasions breaks down the walls surrounding the concept of privacy, and leaves no limits on the meaning of the term. The condition created by such calls is very often annoyance in the common and accepted sense of that term. The TCPA aims at relieving annoyance and not preventing privacy invasions.

Because of the speech implications of this rulemaking, the Commission must consider the constitutional weight of the interest in freedom from annoyance. It should not imagine that an appeal to some amorphous conception of "privacy" will carry the day, because it has not in prior cases.[3] Whether freedom from annoyance holds up as a substantial governmental interest that justifies suppressing commercial speech under *Central Hudson* is an important question requiring First Amendment analysis beyond what Privacilla.org — an organization devoted only to privacy — is prepared to supply.

---

[2] 47 U.S.C. § 227(c)(1).
[3] U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir 1999), cert denied, 520 U.S. 1213 (2000).

Do-Not-Call Listing is Anti-Privacy

There are separate privacy considerations implicated by the Telephone Consumer Protection Act and this rulemaking. Indeed, in do-not-call listing, the Commission is considering instituting a program that encourages Americans to trade away a little privacy for a little peace and quiet. If it is to do so, the choice should be explicit. Government-maintained do-not-call lists are essentially inconsistent with privacy.

As discussed above, information in the hands of government may be deemed categorically unprivate because of the unique power governments have to change the rules under which information is held, including exposing it contrary to the wishes of the data subject. Data held by the private sector can be made subject to legally enforceable limitations that prevent revelation of the data or other undesirable uses. Private parties are also subject to suit under contract law and the privacy torts if they reveal information contrary to agreement or good taste. If governments reveal information in databases they hold, there is no higher authority to which aggrieved parties can appeal.

The points here are not intended to impugn the good intentions or honesty of the Commission, its staff, or any public servant. But wise policy-makers keep in mind that programs created during one era and under one Administration carry forward to different eras and regimes. The purest privacy-protecting intentions of the current generation may not be held by the next. Government data collections persist and they are available to successor Administrations.

In its Privacy Act notice, the Federal Trade Commission indicates plans to collect the telephone numbers of those wishing to decline telemarketing calls. It may also collect dates and times that individuals' telephone numbers are placed on the registry; individuals' specific telemarketing preferences; and other identifying information (e.g., residential zip codes for system record sorting purposes).[4] Assumedly, an FCC do-not-call database would hold similar information.

The FTC's estimate is fairly modest. In order to prevent unauthorized listing of numbers, the FTC may soon enough find itself collecting information regarding the authority of the person electing to place a number on the do-not-call list, such as proof of residency and identity. The Social Security Number would be tempting for this purpose. Additional problems in administration of such a database or additional uses to which it may be put will cause the types of personal information in it to grow along trajectories that are impossible to predict.

The Commission should be aware that information held in government databases in compliance with the Privacy Act is not "private" in a meaningful sense of the word. The Privacy Act's general rule of nondisclosure is subject to at least a dozen exemptions that the data subjects can not prevent or control,[5] including disclosure to Congress and the General Accounting Office, use for investigation without probable cause, and for

[4] FTC Privacy Act Notice, 67 Fed. Reg. at 8985.
[5] *See* 5 U.S.C. § 552a(b).

"routine use." A new "routine use" may be made of personal information if an agency merely places a statement in the *Federal Register* declaring it.[6] New uses, and sharing of information among agencies, are common. In a March 2001 study, Privacilla.org found that Federal agencies commence programs to share personal information about citizens under the Computer Matching and Privacy Protection Act more than once every two weeks.[7]

In essence, when information about a person is held in a government database, he or she does not have legal power to control the use or disclosure of that information. Unable to control disclosure consistent with his or her interests, the user of a government do-not-call database does not enjoy privacy in that information.

If the Commission adopts a do-not-call database, the TCPA requires it to "specify methods for protection of the privacy rights of persons whose numbers are included in such database."[8] If the Commission wishes to treat the TCPA's references to "privacy" as anything more than hortatory, then it must consider and explain the anti-privacy implications of do-not-call listing. Protecting privacy cuts against do-not-call listing because government-held databases and privacy are essentially incompatible.

---

[6] 5 U.S.C. § 552a(e)(4).
[7] *See "Privacy and Federal Agencies:* Government Exchange and Merger of Citizens' Personal Information is Systematic and Routine" (March 2001) <http://www.privacilla.org/releases/Government_Data_Merger.html>.
[8] 47 U.S.C. § 227(c)(3)(K).

The tension between government databases and privacy does not foreclose the institution databases for beneficial public purpose. The Commission may resolve the tension in favor of privacy or in favor of freedom from annoyance, but it cannot do both in a do-not-call database. Such a database should not be characterized as privacy protections but rather as a small diminution of privacy in pursuit of other goals. If the Commission adopts a do-not-call list, it should do so making users aware of the choice they make in using it — abandoning a small portion of their privacy to get some relief from annoyance.

Conclusion

The use of a do-not-call database as discussed in the Telephone Consumer Protection Act is an unsatisfactory way to deliver freedom from the annoyance of unwanted commercial solicitations and privacy at the same time. The difficulty of reconciling the tensions in the Act through a do-not-call list makes other options more attractive. The Commission should focus on technological solutions available and forthcoming in the marketplace. Such solutions can and will empower consumers to suppress communications on precisely the terms they want. Technological and market solutions are not impeded by First Amendment considerations as government regulations are. And they allow those who are most interested in suppressing communications to pay

for it directly in relatively efficient markets rather than shifting the costs to other taxpayers.

Respectfully submitted:

PRIVACILLA.ORG

By: James W. Harper, Esq.
Editor

Privacilla.org
P.O. Box 77576
Washington, D.C. 20013
(202) 546-3701